NUWC-NPT Technical Report 11,790
31 January 2007

Next-Generation Undersea Warfare and Undersea Distributed Networked Systems

Raymond J. Christian
Office of the Director of Undersea Warfare

NAVSEA
NAVAL SEA SYSTEMS COMMAND
Undersea Warfare Center

Naval Undersea Warfare Center
Newport, Rhode Island

Approved for public release; distribution is unlimited.

PREFACE

This report was prepared for the Director of Undersea Warfare at the Naval Undersea Warfare Center (NUWC) in support of the NUWC Undersea Distributed Networked Systems Initiative.

The technical reviewer was Michael J. Pelczarski (Code HQ10A).

The author thanks Robert C. Manke (Code HQ10A) for his salient contributions to this effort.

Reviewed and Approved: 31 January 2007

Peter D. Herstein

Peter D. Herstein
Director, Undersea Warfare

UNITED STATES NAVY

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
31 January 2007

3. REPORT TYPE AND DATES COVERED

4. TITLE AND SUBTITLE
Next-Generation Undersea Warfare and Undersea Distributed Networked Systems

5. FUNDING NUMBERS

6. AUTHOR(S)
Raymond J. Christian

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Undersea Warfare Center
1176 Howell Street
Newport, RI 02841-1708

8. PERFORMING ORGANIZATION REPORT NUMBER
TR 11,790

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

Since the early 1990s, the undersea warfare (USW) community has experienced dramatic changes in its operational, technical, and business climates. The changes are expected to continue and perhaps accelerate—leading to significant new demands for USW capabilities. Because many of the currently proposed new capabilities are just an expansion of Cold War ways, it is valuable to lay the groundwork for what is being termed "Next-Generation Undersea Warfare." The USW paradigms of the past, which included single-platform missions, long time scales, and Cold War-era ocean dimensions, are being substantially replaced by complex joint force and distributed, networked littoral operations with significantly decreased tactical operating areas and times. Central to Next-Generation USW is knowing that operating in the undersea domain is difficult to master and comes with a relatively high entrance cost in the form of doctrine, organization, training, materiel/technology, leadership, personnel, and support facilities. Operating in the undersea domain, however, has significant inherent advantage for staging and conducting joint force littoral operations. This report presents the rationale, inherent advantages, and implications of Next-Generation USW.

Additionally, undersea distributed networked systems (UDNS)—consisting of sensors, unmanned vehicles, platforms, weapons, command/control and, most important, human systems networked to create effects that can be summoned for advantage by the clever warfighter—promise to be a key enabler for Next-Generation USW. This report defines and articulates the nature of UDNS for the technologist and the warfighter. The goal is to help system developers and engineers sort out new system functions and relationships that may be added to the future seabed-to-space theater-level combat system and generate a warfighting advantage. What is presented is the notion that engineering UDNS as a complex system will likely be one of the next great challenges for the USW technical community—a challenge that must incorporate new methods and processes of evolutionary engineering.

14. SUBJECT TERMS
Undersea Warfare
Complex Systems Engineering
Undersea Distributed Networked Systems
Evolutionary Engineering

15. NUMBER OF PAGES
62

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT
Unclassified

20. LIMITATION OF ABSTRACT
SAR

TABLE OF CONTENTS

Section **Page**

LIST OF ILLUSTRATIONS

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

AIP	Air-independent propulsion
AOU	Area of uncertainty
ASCM	Antiship cruise missile
ASDS	Advanced Swimmer Delivery System
ASUW	Antisurface warfare
ASW	Antisubmarine warfare
BDA	Battle damage assessment
C^2	Command and control
CG	Guided missile cruiser
CONOPS	Concept of operations
CSG	Carrier strike group
CVN	Aircraft carrier (nuclear propulsion)
DDG	Guided missile destroyer
DME	Deploy, manage, and exploit
DMER^5	Deployment, management, exploitation, redeployment, refueling, repositioning, replacement, recovery
DNS	Distributed networked system
FYDP	Future year defense plan
I&W	Indications and warning
IPB	Intelligence preparation of the battlespace
ISR	Intelligence surveillance reconnaissance

LIST OF ABBREVIATIONS AND ACRONYMS (Cont'd)

LCS	Littoral combat ship
LPD	Amphibious transport dock
M&S	Modeling and simulation
MIW	Mine warfare
OMFTS	Operational maneuver from the sea
Pfa	Probability of false alarm
R^5	Redeployment, refueling, repositioning, replacement, and recovery
ROE	Rules of engagement
RSTA	Reconnaissance, surveillance, target acquisition
STOM	Ship-to-objective maneuver
TTP	Tactics, techniques, procedures
UAV	Unmanned air vehicle
UDNS	Undersea distributed networked system
USV	Unmanned surface vehicle
USW	Undersea warfare
UUV	Unmanned undersea vehicle
UV	Unmanned vehicle

NEXT-GENERATION UNDERSEA WARFARE AND UNDERSEA DISTRIBUTED NETWORKED SYSTEMS

1. INTRODUCTION

Since the 1990s, the undersea warfare (USW) community has experienced dramatic changes in its operational, technical, and business climates. Such changes are likely to continue—and even accelerate, leading to significant new demands for USW capabilities. The USW paradigms of the past, which included single-platform submarine, antisubmarine warfare (ASW), and mine warfare (MIW) missions; long time scales; and ocean dimensions of the Cold War-era ocean dimensions, are being substantially replaced by complex joint force and distributed littoral operations with significantly decreased tactical operating areas and times. Yet, many of the proposed "new" USW capabilities are merely expansions of the Cold War methods and strategies consistent with traditional definitions and views of USW.[1, 2]

To keep pace with the dynamic USW environment of the 21st century, it is valuable to lay the framework for a new USW mindset that has recently been termed "Next-Generation USW" by the Naval Undersea Warfare Center's Technical Director.[3] Essential to the success of Next-Generation USW is acknowledging that operating in the undersea domain is difficult to master and comes with a relatively high entrance cost in the form of doctrine, organization, training, materiel/technology, leadership, personnel, and support facilities. Equally important is knowing that the undersea battlespace has inherent advantages for staging and conducting joint force littoral operations. Additionally, this mindset recognizes that the implications for the submarine platform are significant and that the submarine, having been relatively isolated in the past, may well bring significant new capabilities to the joint distributed and networked force.

Undersea distributed networked systems (UDNS), consisting of sensors, unmanned vehicles, platforms, weapons, command and control (C^2), and, most important, human systems networked to create advantage for the clever warfighter, will be a key enabler for Next-Generation USW. The complexity of UDNS relative to the networking of current systems, however, has resulted in either (1) concepts being developed without an understanding of the military value/payoff or (2) little innovation being attempted because the problem is considered too difficult.

This report establishes the framework for the Next-Generation USW mindset and defines the nature of UDNS for the technologist and the warfighter. Specifically, this report (1) presents the rationale, inherent advantages, and implications of Next-Generation USW; (2) describes UDNS as a key enabler for the Next-Generation USW; and (3) explains why engineering UDNS as a complex system is a challenge for the USW technical community that must co-evolve with warfighter concepts of operations. It is hoped that this report will help system developers sort out new system functions and relationships that may be added to the "realm of the possible" for the Next-Generation USW warfighter.

2. NEXT-GENERATION UNDERSEA WARFARE

2.1 STRATEGIC LANDSCAPE

The current and future national security landscape is being defined by the September 11 attack on this nation and its subsequent engagement in the War on Terror. National strategic security documents call on the military to be prepared to prevail against threats posed by a wide range of adversaries—from states to non-state actors operating within the maritime commons who may or may not have weapons of mass destruction.[4, 5] The 2006 *Quadrennial Defense Review*[6] lays out the force planning construct for a new level of joint service and coalition force teamwork that is capable of coordinated joint military operations among the services while transforming forces "in stride" to field new capabilities in distributed operations for agility, decisiveness, and integration in the littoral battlespace:[6]

> Joint maritime forces, including the Coast Guard, will conduct highly distributed operations with a networked fleet that is more capable of projecting power in the "brown and green waters" of coastal areas. . . .
>
> . . . Undersea capabilities, both manned and unmanned, will use stealth, survivability, endurance, payload size and flexibility to complicate foes' planning efforts and strengthen deterrence.

Thus, future USW capabilities will be constructed within the context of networked "joint force interdependence" and naval force structure constraints[7, 8] to deal with a wide range of adversaries and battlespace environments. The U. S. Navy has promulgated a strategic plan,[9] an operations concept,[10] and an ASW concept of operations[11]—all of which have adopted "Sea Power 21" as the framework for how the Navy will organize, align, integrate, and transform to a distributed, networked maritime force. In short, distributed networked operations[12] will shape the evolution of USW and its associated technology and business operations beyond the traditional enabler role to be more closely integrated with other warfare areas.

The future defense themes are clear, and the implications for Next-Generation USW are significant: advantage is found in full-spectrum combat power generated within and projected from the waters beneath the surface.[13] Next-Generation USW is evolving to be warfare from under the sea supporting, enabling, and integral to distributed networked joint forces that will be expeditionary, adaptable, and responsive to a broad set of missions and tasks that support the defense strategy. To deter and defeat opponents who will increasingly employ deception, surprise, and asymmetric and unconventional methods to achieve their objectives, these joint forces must be able to (1) rapidly deploy and surge forward and (2) employ versatile combat capabilities with flexible multimission force packages. Operations must be fully coordinated and interoperable, enabled by a networked architecture to permit collaborative planning and decentralized execution, resulting in dramatically compressed decision cycles. The Navy's Next-Generation USW capabilities must be consonant with the capability trends of the greater joint force: (1) increased speed of maneuver, (2) routine precision, (3) networked awareness, (4) distributed sensing, (5) greater persistence, (6) flexible payloads, and (7) integrated deployment, management, exploitation, redeployment, refueling, repositioning, replacement, recovery (DMER[5]).

2.2 NEXT-GENERATION USW: THE RISK CALCULUS

The Navy will require sufficient littoral sea dominance to enable viable sea basing from relatively large, deep-ocean sanctuaries to near-shore "global Fleet stations." These sea-based forces must be capable of adaptive force packaging in support of joint force missions. Littoral regions where naval operations are conducted traditionally involve near-shore shallow and deep waters. The littoral region expands considerably when the range at which adversarial seaborne and/or land-based forces can influence each other increases because of greater sensor and weapon envelopes. Threats to the ability to rely on the availability of an in-theater, shore-based infrastructure from which joint combat power can be launched is driving the United States to sea-based force options, both nearshore and offshore, that can seize and sustain battlespace access and project lethal and nonlethal power when required.[10]

The proliferation of military systems, information sources, processing and communication technologies, and disruptive technologies is worldwide. Potential adversaries are increasingly capable of developing or purchasing multidimensional, anti-access capabilities to keep U.S. Naval forces from being effective in the littoral environment; they are creating risks that are driving changes to the battlespace calculus.

Proliferating technologies and weapons include modern air defenses, air-independent propulsion (AIP) submarines, third- and fourth-generation antiship cruise missiles (ASCMs), modern torpedoes and advanced mines, traditional mines, fast patrol boats, ballistic missiles, and reconnaissance, surveillance, target acquisition (RSTA) systems. Certain theaters have threat submarines and fast inshore attack boats that can affect the warfare calculus by presenting a large number of credible threat vectors. These platforms can employ ASCMs, wake-homing torpedoes, high-speed torpedoes, and advanced mobile mines to deny access to sea-based forces. The threat's area-denial, littoral, undersea component can also be easily expanded to include minisubmarines, unmanned undersea vehicles (UUVs), and undersea surveillance systems—all of which are readily available on the open market.[14, 15] Air, surface, and undersea anti-access capabilities are obtainable in varying degrees if an adversary sees a sufficient cost-to-benefit ratio and is willing to make the investment.

The net effect of the current and emerging threats is increased risk to U.S. and coalition forces. For example, in the absence of capability and/or capability improvements, both the composite detection envelope of a typical carrier strike group (CSG) for diesel-electric or AIP submarines and the distance at which CSG assets must be positioned relative to each other to maintain the integrity of an ASW screen decrease as threat submarine acoustic stealth increases. Moreover, as threat submarine ASCM ranges increase, joint force access to the littoral battlespace will be significantly challenged.

Over the years, the traditional U.S. Navy response to submarine acoustic-quieting trends and reduced ASW detection envelopes has been the (1) development and fielding of larger or improved sensing arrays (primarily passive acoustics) to extend the search ranges of tactical platforms and cueing assets and (2) examination and development of active, multistatic, and nonacoustic detection capabilities. These traditional responses are seemingly insufficient for pacing the threat in the long term. Further complicating the problem are conditions associated with littoral operations: dynamic environments, heavy clutter/false targets, masking of targets of interest, and harsh acoustic conditions. In addition, current force structure planning is challenged to provide the necessary increased numbers of platforms equipped with relatively short-range sensors to address capacity and capability gaps in the decades ahead.[7, 8, 15] The net result is added risk for (1) U.S. Navy detection and engagement capability at tactically desirable distances, (2) effective search rate/time scale capabilities for areas of interest, and (3) joint force operations.[11, 13, 16]

Professor Wayne Hughes of the U.S. Naval Postgraduate School, in assessing naval risk, argues that a naval force must be tactically stable if it is to have utility.[17] The concept of tactical stability compares the combat power of a force to its survivability (see figure 1). In a tactically stable force, combat power and survivability are approximately equal. If combat power is greater than survivability, a force becomes tactically unstable because it grows risk-averse. A force whose survivability grows at a rate greater than its combat power is of little value because it cannot do much more than survive. Hughes[17] contends that three primary factors govern risk-aversion: (1) loss of human life is possible, (2) highly capable, multimission platforms (for example, CVNs, CG/DDGs, LPDs) constitute a disproportionately large percentage of the force's combat power, and (3) replacement cost of even one such platform is very high.

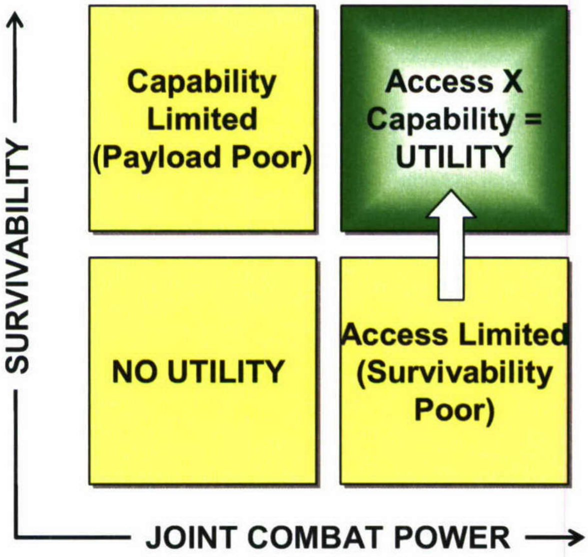

Capability Limited (Payload Poor)
Access X Capability = UTILITY
NO UTILITY
Access Limited (Survivability Poor)
SURVIVABILITY
JOINT COMBAT POWER

Figure 1. Concept of Tactical Stability

A tactically unstable force becomes marginalized because its commanders are inhibited in its use except when the most vital of national interests are at stake. The increasing risk to air-based forces and surface sea-based forces creates a tactical instability, and the joint commander will likely seek options to exploit the undersea environment where greater survivability can exist to help secure access, to get in close for certain missions (such as intelligence preparation of the battlespace (IPB), strike, antisurface warfare (ASUW)), and manage the overall tactical stability. The value proposition of Next-Generation USW addresses this risk context for the joint force commander.

Theater risk management, then, will likely have to exploit the undersea domain for advantage in the following ways, especially when covertness, proximity, and persistence are necessary attributes:

- Create the pervasive sensing and networking sufficient for sustained littoral awareness—especially against key antiship and antiair threats and activities associated with the transition to war.

- Replace force-on-force with distributed force and massed effects. Sufficient platform numbers and speed for rapid concentration of mass must be summoned by the theater commander. Combat power distribution across manned and unmanned platforms, above and below the sea surface, is an approach for capability reach that creates options for risk tolerance and robustness.

- Create a networked total force to share awareness and conduct coordinated network-centric operations enabling (1) force dispersal, hiding, and greater standoff range, (2) surprise pre-emptive, retaliatory, containment attack on the adversary from unpredictable sources, (3) more rapid, distributed employment decisions, (4) greater economy of force, and (5) greater actual firepower from joint and allied forces.

- Create and exploit the adversary's tactical instability through disruption, desynchronization, and destruction of key high-threat, low-density forces, RSTA, and C^2.

2.3 NEXT-GENERATION USW: DESIRED CAPABILITIES

Sea Power 21 underscores the need for distributed networked force capabilities, thus fostering the need for a strategy that integrates air power with sea power. Major components of the Sea Power 21 philosophy include sea basing, sea strike, sea shield, and FORCEnet.

1. Sea Basing - requires strategic positioning of the joint assets afloat nearshore and offshore, offensive and defensive power projection, integrated C^2, joint logistics, and accelerated timelines.

2. Sea Strike – requires persistent intelligence surveillance reconnaissance (ISR), time-sensitive strike, covert strike, and electronic warfare operations/information operations.

3. Sea Shield - demands the ability to forcibly gain access when required to ensure sea/littoral superiority, theater air-missile defense, and homeland defense.

4. FORCEnet – must bring sea basing, sea strike, and sea shield together via expeditionary, multitiered, sensor/weapons networking, distributed/collaborative C^2, and dynamic and multipath survivable networking.[12]

Under Sea Power 21, Next-Generation USW, will have operational demands to provide the following capabilities that go beyond those associated with traditional submarine, ASW, and MIW operations:

- Provide a flexible and scalable capability to rapidly destroy, degrade, negate, or avoid threats (for example, submarines, minisubmarines, UUVs, mobile mines) as appropriate to the operational and/or tactical objectives and situation.

- Provide a capability to conduct operations in highly contested areas in the presence of a multitude of potential anti-access forces. Flexibility is desired via covert and overt capability options.

- Provide a capability that enables the conduct of simultaneous operations in multiple geographically dispersed areas of interest, within an overall operational area of significance and within operationally and tactically significant time scales. Tactical areas of significance may range from inter-island choke points to coastal ocean-basin dimensions. Some or none of these areas may contain pre-installed warfare capability. Time scales may range from prehostilities with weeks of preparation to hostility where only hours are available.

- Provide a capability to conduct ASW, ISR, IPB, indications and warning (I&W), and mine countermeasure operations in parallel with other warfare operations.

- Provide a capability to rapidly deploy, manage, and exploit (DME) offboard sensors and to rapidly redeploy, refuel, reposition, replace, and recover (known as R^5) nonexpendable sensors.

- Provide a capability to rapidly deploy, redeploy, refuel, reposition, replace, and recover offboard weapons systems.

- Provide a capability to conduct wide-ranging operations from under the sea, such as (1) disruption of C^2 and/or cueing for the adversary's submarine, (2) detect, track, and trail prehostilities in geographic areas of interest, (3) in-stride/transit area clearance and neutralization of submarines, mines, UUVs, and (4) area denial/protection of U.S. battlespace.

- Provide a capability that reduces U.S. Navy platform susceptibility to ASCM and torpedo attack from the shore, air, surface, and undersea.

- Provide a covert, in-close, reconfigurable ISR in support of an I&W that keeps the joint force ahead of the decision cycles of the adversaries.

- Provide a rapid mission-kill ASUW against multiple threat axes.[16]

2.4 NEXT-GENERATION USW: OPERATIONAL CONCEPTS

Next-Generation USW operational concepts must explore new distributed networked force paradigms that have the potential to significantly improve the Navy's warfighting capability by providing total solutions—rather than point solutions—to the problem. Effective Next-Generation USW operational concepts must address the following elements:[11, 13, 16]

- Operational flexibility for rapid and decisive action for the destruction, degradation, negation, and/or avoidance of the adversary's mobile undersea threats (submarines, minisubmarines, and UUVs).

- Decisive undersea control through a change in the spatial and temporal aspects of the undersea competition.

- Integration of distributed, large-area offboard sensors and weapons with unmanned/autonomous vehicles and manned platforms.

- Denial of the enemy's ability to gain access to U.S. or allied power projection battlespace.

- Covert and clandestine battlespace environmental and operational characterization for long-term battlespace preparation and for around-the-clock, real-time situational awareness and the integration of these data into USW (that is, full-spectrum access operations).

- Synergy of access forces, force protection, and power projection forces in the conduct of joint missions.

- Determination of the level of risk (via analysis tools and decision aids) at a given point, considering mission, tasks, rules of engagement (ROE), objectives, and other appropriate factors.

- Manning within available levels.

Next-Generation USW operational concepts promote the capability of anticipation and prediction of enemy movement (above and below the surface) and should incorporate weaponeering capability that articulates "if I can see you, I can hit you" as a genuine risk to the adversary regardless of the threat's maneuver or action.

Future operational concepts must be built on two primary paradigm shifts centered on relationships with the warfighter (figure 2). The first paradigm shifts from the current sensor-poor condition, where the sensor-to-warfighter ratio is relatively low, to sensor-rich conditions, where the sensor-to-warfighter ratio increases greatly. Significant numbers, perhaps thousands, of autonomous distributed sensors will need to be managed by modest numbers of warfighters to support operations. This paradigm shift will enable the conduct of avoidance and/or ASW prosecution operations, where detection, classification, localization, tracking, and neutralization of adversary undersea threats can be accomplished at a distance from manned platforms.

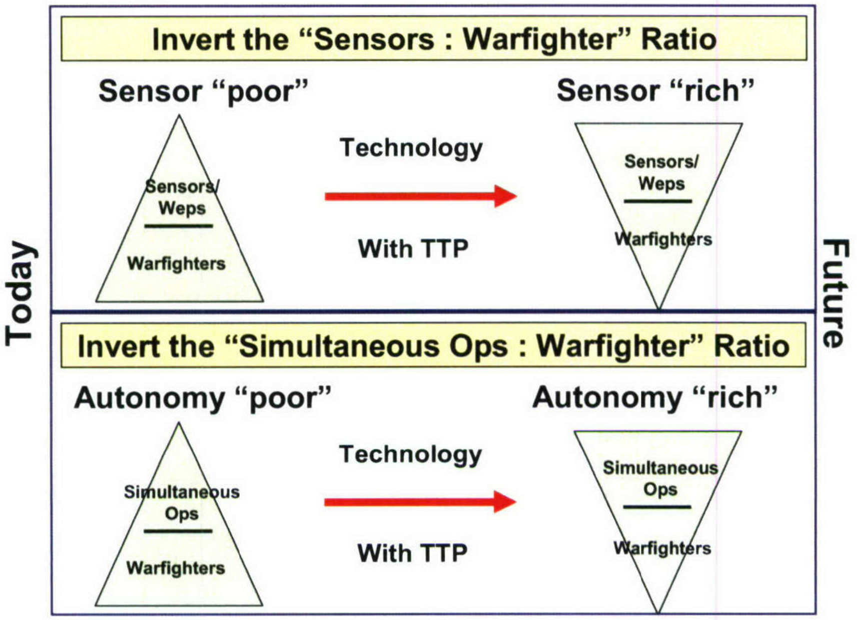


Figure 2. Paradigm Shifts Shaping the Warfighting Operations

The second paradigm shift relates to the utilization of autonomous and/or unmanned vehicles, significantly enhancing the ability to conduct simultaneous operations in multiple areas of interest with the same or a smaller number of warfighters. The conduct and control of parallel warfare operations reduce the timeline in a manner of the warfighter's choosing to overcome the enemy's undersea capability. The nature of the paradigm shifts in the joint operations context, by necessity, will demand tight alignment of the joint force commander's theater strategic goals and Next-Generation USW tactical operations.

A notional ASW from-under-the-sea concept of operations (CONOPS) discussed in appendix A shows how the new methods and technologies could come together in a traditional USW mission area in such a way that UDNS enables avoiding force-on-force engagement.[13] Integrating the elements of operational art with the technological realm-of-the-possible illustrates the nature and the potential strength of the Next-Generation USW operational concepts. The illustrative CONOPS focuses on ASW support to the joint force and is based on stressing force-space-time dimensionality.

Next-Generation USW operational concepts must evolve within the realities of the capacity and capabilities of future naval platforms. Affordability is in the forefront of current Navy investment strategy and is a key driver for future force structure, capability improvements, sustainability, and manning levels.[7, 8] Noteworthy is the argument that affordability is also a key driver supporting the value proposition for Next-Generation USW. Specifically, affordability constraints that lead to fewer platforms with greater joint combat power will yield the tactical instability and associated risk described in section 2.2. Investment in Next-Generation USW capabilities is imperative for managing the risk associated with the realities of the threat landscape and more modest, resource-constrained force structure and capabilities.

Whatever future force structure materializes, submarine, surface, and air platforms will probably be elements of the UDNS, along with mobile and fixed unmanned systems, shore sites, and space assets. Platforms will take on new roles as their joint, interdependent relationships with other parts of the theater-level combat subsystems evolve with time. It will be shown later in this report that the exact role and value of future platform systems to Next-Generation USW cannot be predicted *a priori*; however, platform attributes from the submarine and littoral combat ship (LCS) in the current force-structure planning appear to be key enablers to Next-Generation USW.

Speed, payload, and endurance design tradeoffs in the first builds of the LCS are complementary with supporting the Next-Generation USW desired capabilities described in section 2.3.[18] The significant numbers of LCSs and modest combat power density that are being planned are consistent with efforts to avoid tactical instability (see section 2.2). The specific warfighting functions delivered by the payload modules remain to be seen, but the LCS concept appears to be poised to offer value in the management of the future USW risk calculus.

The attributes of U.S. submarines with their stealth, speed, endurance, and payload capacity also offer promising unique roles in Next-Generation USW—roles that will build upon traditional capabilities to exploit the undersea domain and project combat power from under the sea. Appendix B discusses the implications of Next-Generation Warfare imperatives for the submarine platform with the overarching view that platform payload augmentation will be the hallmark of the 21st century submarine, enabling it to work with unmanned vehicles as a key joint asset for Next-Generation USW.

3. UDNS: ENABLER FOR NEXT-GENERATION USW

3.1 DEFINITION AND DESCRIPTION

Distributing combat power for Next-Generation USW operations will demand networked systems with a heterogeneous mix of elements ranging from a few to a few hundred that are typically well connected with both strong and weak interactions between nodes. UDNS will have to be engineered to include scalability of military response, mobility matched to the scale of operations, adaptation, persistence for continuous operations that avoid disruptive logistics tails, spatial dispersion, and low cost-to-effect ratio. The vision of such a system can be more readily perceived by thinking of UDNS in terms of the following unpublished working definition developed by Cares, Christian, and Manke, which is in keeping with their concepts published in NUWC-NPT Technical Report 11,366:[19]

> In its future state, the UDNS is a large group of interacting, independent, and diverse elements and connections that, based on system-induced information transactions, respond with or without central direction in varied, yet coherent, aggregate behavior appropriate to the USW conditions.

In an operational sense, the UDNS is the sensors, unmanned vehicles, platforms, weapons, C^2 and, most important, human systems networked to create effects that can be used to advantage by the clever USW warfighter. Thus, UDNS in the far-term can be viewed and engineered as a complex adaptive system.

A basic description of the functions, characteristics, and design goals for generic distributed networked systems (DNS) applicable to UDNS is provided in appendix C.[19] Key to understanding UDNS is the notion that system functions (for example, sensing, transporting, and networking) that have to be performed in the battlespace can be decoupled from the large platform functions of today. While platforms are an important part of the overall system, the focus turns to marshaling functional effects from several subsystems that have sufficient spatial separation integral to the functionality.

The future UDNS will not be built directly from the legacy systems in today's Navy; rather, a notional three-phase evolution of UDNS is envisioned: near-term UDNS-1, mid-term UDNS-2, and far-term UDNS-3. A notional three-phase evolution will have to occur within incremental and transformational development trajectories as noted in figure 3. The incremental development is closely associated with improvements to legacy systems in the program of record; the transformational development will be governed by disruptive innovations from technologists and warfighters that "change the calculus" and are afforded greater risk.[20] Both trajectories are important and must occur concurrently; they must, however, be governed by different rule sets.[21]

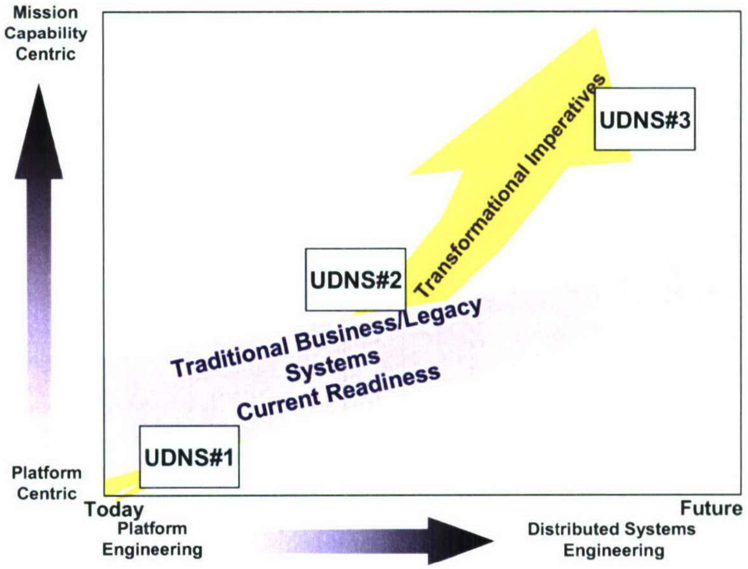

Mission Capability Centric
Platform Centric
UDNS#1
UDNS#2
UDNS#3
Transformational Imperatives
Traditional Business/Legacy Systems
Current Readiness
Today
Platform Engineering
Future
Distributed Systems Engineering

Figure 3. Multiphase Evolution of an Integrated DNS

Today's near-term UDNS-1 is identified by a small number of elements with strong physical connections; the force is in the early stages of networking, but has limited ability to distribute combat power. The risks of tactical instability (see section 2.2), therefore, are inherent in today's naval forces. UDNS-1 consists of existing platforms with some degree of integration from established links and C^2 necessary to exploit the current capabilities. UDNS-1 relies primarily on centralized decision-making.

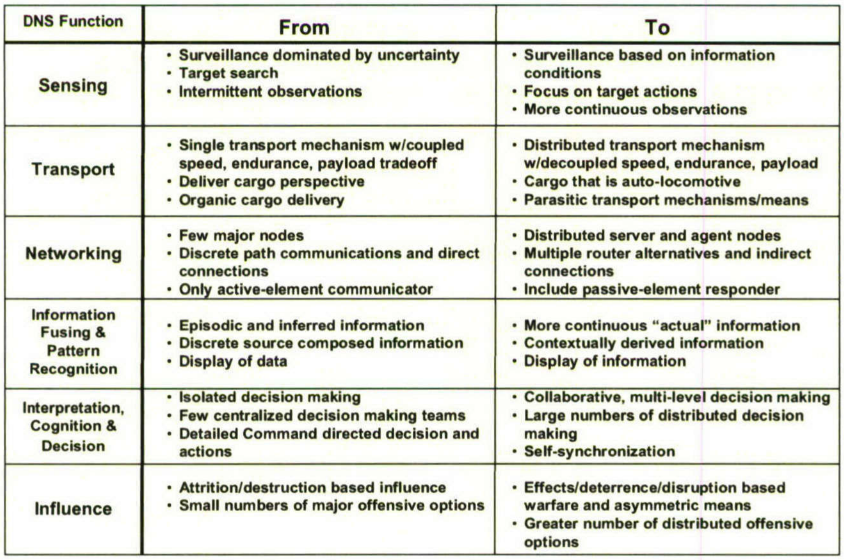
In the mid-term, that is, in about a decade just beyond the Future Years Defense Plan (FYDP) Program of Record, UDNS-2 will likely evolve by adding unmanned vehicles and offboard systems to the growing network to achieve a greater capability of distributing the combat power. The realities of future force-level constraints[7, 8] suggest that today's platforms are tomorrow's platforms (across the FYDP), only fewer in number; therefore, distribution of combat power will necessitate augmentation with offboard devices. Offboard devices, for the most part, must emanate from existing platforms, and networking must evolve beyond physical links. UDNS-2 must have decoupling of sensors, C^2, and response systems. Semi-automated information management is required and must be designed from an information-engineering basis. Operational tactics, techniques, and procedures (TTP) and CONOPS will have to adapt to take advantage of the new possibilities.

In the far-term, well beyond the FYDP, UDNS-3 is projected to emerge as having a much larger number of elements—the majority of which will not be physically connected to the small number of larger parts (for example, platforms). It is likely that most parts will not be physically connected to any part. UDNS-3 will be characterized by a mix of old and new platforms, with the number of offboard devices far exceeding the number of platforms. Autonomous collective system behavior will be necessary for realizing the paradigm shifts described in section 2.4 and enabled by plug-in network components and automated information management. Thus, UDNS-3 will likely have characteristics of a complex adaptive system.

3.2 DNS PARADIGM SHIFTS

UDNS-2 and UDNS-3 will be characterized by what they do for the warfighter in enabling new ways of gaining advantage in the battlespace. UDNS paradigm shifts provide information on critical system functional issues and challenges for enabling new CONOPS. The generic DNS functions described in appendix C can be put in the context of a Next-Generation USW UDNS-3, resulting in plausible tactical and system paradigm shifts relative to the traditional USW of today. These paradigm shifts are summarized in table 1 and explained in paragraphs 3.2.1 through 3.2.6.

Table 1. Functional Paradigm Shifts Enabled by DNS



DNS Function	From	To
Sensing	• Surveillance dominated by uncertainty • Target search • Intermittent observations	• Surveillance based on information conditions • Focus on target actions • More continuous observations
Transport	• Single transport mechanism w/coupled speed, endurance, payload tradeoff • Deliver cargo perspective • Organic cargo delivery	• Distributed transport mechanism w/decoupled speed, endurance, payload • Cargo that is auto-locomotive • Parasitic transport mechanisms/means
Networking	• Few major nodes • Discrete path communications and direct connections • Only active-element communicator	• Distributed server and agent nodes • Multiple router alternatives and indirect connections • Include passive-element responder
Information Fusing & Pattern Recognition	• Episodic and inferred information • Discrete source composed information • Display of data	• More continuous "actual" information • Contextually derived information • Display of information
Interpretation, Cognition & Decision	• Isolated decision making • Few centralized decision making teams • Detailed Command directed decision and actions	• Collaborative, multi-level decision making • Large numbers of distributed decision making • Self-synchronization
Influence	• Attrition/destruction based influence • Small numbers of major offensive options	• Effects/deterrence/disruption based warfare and asymmetric means • Greater number of distributed offensive options

3.2.1 Sensing

Technology development in micro-engineering and fabrication, computing, energy storage, and target classification enables fields of in-close sensors yielding near-continuous information flows from the littoral undersea environment. The fields could have hundreds or thousands of multiple phenomenology sensors and physical measurement merged with computing, resulting in a sensor being an information generator for the network. Sensors will need employment capability from air, surface, subsurface, and unmanned vehicles. UDNS sensing enables tactical sensing strategies that shift from traditional surveillance and target search dominated by relatively large uncertainty and intermittency to more continuous monitoring-like surveillance based on the information conditions of the area of interest focused on target actions (or inaction).

3.2.2 Transport

Advances in ocean interface technologies (for example, unmanned vehicle handling, launch, and retrieval) and autonomous vehicle behavior control algorithms enable a theater fleet of in-close and stand-off payload delivery vehicles. Distributed transport mechanisms from different modalities (air, surface, subsurface) allow some decoupling of the current constraints of speed, endurance, and payload. Many of the medium-to-light payloads will likely have designed modularity enabling a shift from an organic cargo delivery with central logistics platforms to payload delivery from a variety of transport vectors, accreting payload deliveries based on response to the changing needs of the warfighter.

3.2.3 Networking

The difficult air-sea boundary is a key factor in Next-Generation USW telecommunications, acoustic communications, and networking. Networking components will likely have combined use of node memory, mobility, and FORCEnet joint interoperability while using adaptive communications paths to negotiate the large variance between water and air mediums of transmission. Paradigm shifts are enabled, going from a few major network nodes with discrete path communications and direct connections to many nodes acting as a distributed server with multiple router alternatives.

3.2.4 Information Fusion and Pattern Recognition

Information technologies and the maturing discipline of informatics take the current episodic, inference-based USW information, where the focus is on displaying data that can be retrieved from the battlespace, to a paradigm of more continuous information that is contextually driven and displayed. The human decision needs will likely be engineered into the information management from the first design of the information systems.

3.2.5 Interpretation, Cognition, Decision

Technologies that include real-time information reach-back (for example, telepresence), software-agent-tasking, decision-management logic, and machine learning allow for a scalable, adaptable, distributed, theater decision team. The current isolated decision-making from a few centralized epicenters will have to shift to collaborative multilevel decision-making. This shift should enable larger numbers of parallel synchronized decisions to be executed rapidly with greater understanding of intent.

3.2.6 Influence

Advances in areas such as competent munitions, tagging, inertial guidance, and nonlethal weapons should enable a shift from the current destruction-based USW (principally from modest numbers of large torpedoes) to a greater number of distributed offensive options that will include a variety of lethal and nonlethal effects. The adversary may see a number of weapon threat-vectors that force changes in behavior leading to deterrence and disruption of mission.

In addition, there will likely need to be a shift to more global, distributed, networked test and evaluation and readiness infrastructure to support the UDNS. The future support functions must be designed to meet end-to-end spiral development needs (from concept development to in-service engineering) with integration of laboratory-to-theater, on-demand, turn-key measurement and analysis. The theater-level UDNS demands a national U.S. Navy and joint laboratory testbed capable of scalable interplay between the joint environment, machine simulation, and the human. The capability will likely include obsolescence engineering paradigms applied to small numbers of mature, theater-driven prototypes, enabling adaptivity and progress to be made in the midst of noncommittal acquisition. The future supporting infrastructure will be important for system-development risk management within an evolutionary engineering framework discussed in section 4.

3.3 OPERATIONAL CAPABILITIES TRADESPACE

The full dimension of operational capabilities tradespace has to be considered for UDNS design. Figure 4 shows an example of conceptual tradespace profiles across the ASW kill chain; it illustrates what is necessary to provide options for the warfighter in risk reduction.

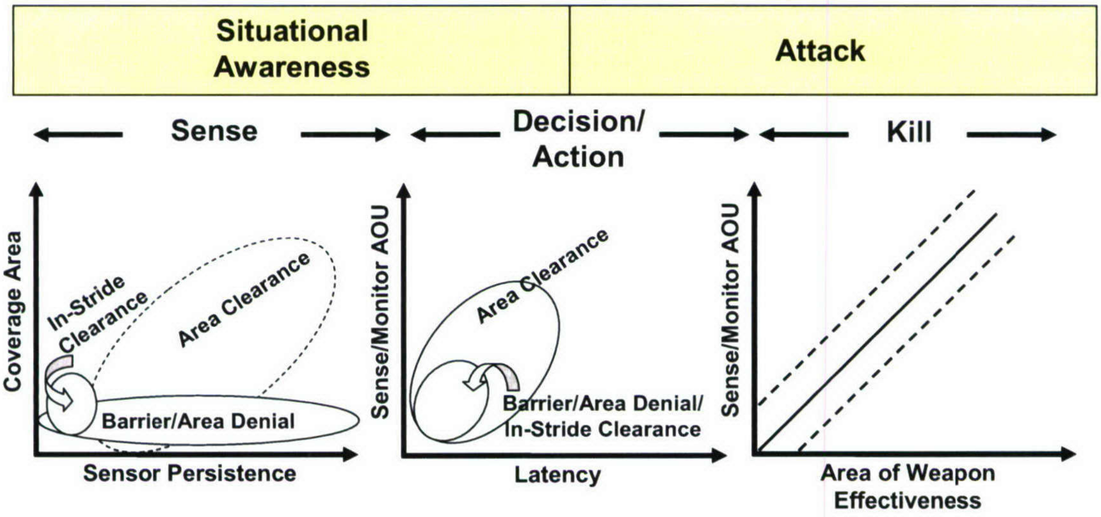


Figure 4. Example of Conceptual ASW Kill Chain Tradespace

The UDNS sensor portfolio will likely need some large-area clearance and long-persistence capability with associated technical and DMER[5] constraints; the portfolio could also have sensor systems that are short-lived with reduced area coverage for barrier or in-stride clearance operations, but with more favorable technical and DMER[5] characteristics for certain contingencies and CONOPS. Similarly, the C^2 weapon system portfolios may need a range of monitoring/sensing areas of uncertainty (AOUs) appropriate to the decision latencies and weapon area of effectiveness to provide the requisite options to the warfighter. So, for example, weapon-target pairing becomes a useful and plausible, distributed operations support function for UDNS with the appropriate combination thresholds of sensing AOUs, decision latency, and weapon area of effectiveness.

To some extent, UDNS-1 can be described in some detail; however, the complex nature of UDNS-2 and UDNS-3 preclude such detailed descriptions—a situation that is frustrating to many developers and leads to the tendency for incremental improvement designs to be identified as "The UDNS" (UDNS-2 or UDNS-3). To avoid this frustration and tendency, UDNS characteristics, attributes, and design goals must be used by both incremental and transformational design engineers of sensors, networks, weapons, C^2, and transport subsystems to innovate with proposed functionality. Sometimes the innovation will fill a niche for the warfighter; at other times, the innovation can be so comprehensive that it influences the theater-level system behavior. Achieving these different levels of innovation requires that the systems engineering community employ different evolutionary methods of end-to-end development and integration.

4. ENGINEERING UDNS FOR NEXT-GENERATION USW

4.1 EVOLUTIONARY ENGINEERING

Realizing a UDNS for the military user will demand that rigorous systems engineering disciplines be applied in a context that is more complex, distributed, and networked than what was used for the USW systems of the past. The purpose of systems engineering remains the same: to increase a system's probability of functioning effectively and reducing the risk of failure. As a starting point for engineering development, variants of the generic systems engineering process begin with requirements analysis and proceed through the design, implementation, and testing phases as shown in figure 5, where the solid arrows show primary dependency and the dashed arrows indicate options if testing is required for all phases.[22, 23]

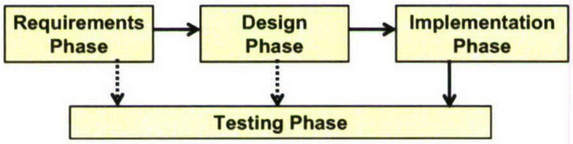


Figure 5. Generic Systems Engineering Process

The engineering community is recognizing that conventional systems engineering strategies of relatively deterministic system planning, analysis, and design are not appropriate for complex systems such as the UDNS. When systems become highly complex, complicated behaviors can emanate from any one of a number of factors: large numbers of elements, large numbers of relationships within the system, nonlinear and discontinuous relationships, and uncertain characteristics of elements and relationships.[23, 24, 25] For these systems, requirements become intrinsically evolutionary because they must operate in a dynamic, unpredictable environment; moreover, because these systems support nondeterministic human decision-making processes, they cannot be specified *a priori*. The systems engineering development process changes the user's perception of what is possible, leading to changes in the requirements. The traditional process (see figure 5) accommodates some feedback from testing to the design and implementation phases; however, requirements are fixed, and any feedback involves revised interpretation of the user requirements versus revision of the requirements.

It is evident that adaptations to the traditional systems engineering process are needed for UDNS. Bar-Yam[26] and others[24, 25, 27, 28] draw on two theorems to guide the strategies for engineering complex systems. The first theorem is Ashby's Law of Requisite Variety, which correlates the complexity of engineered systems with the complexity of the task being demanded of the system. Ashby's law points to the requirement for variety in complex system regulation versus the simple system's reductionism methods of centralized optimization control. The second theorem is one that proves that adequate functional testing, including modeling and simulation (M&S), of complex engineered systems is not possible. This theorem acknowledges the phenomenon of behavioral complexity, where the complexity of the system's functions is much larger than the system, which is already complex in nature and subject to environmental influence with nondeterministic macroscopic response.

As UDNS complexity increases, the engineering effort shifts from the system components to the component dynamics and the coordination and relationships between components. UDNS-2 and -3 will need an evolutionary engineering approach that emphasizes empirical methods. The traditional requirements-based system engineering of *a priori* design-and-build with applied standards and protocols is inadequate for UDNS-2 and UNDS-3 development. UDNS-2 and -3 development requires evolutionary engineering, which will generate hypotheses on how changing system elements and configurations could result in significant progress toward an operational requirement. For Next-Generation USW, the UDNS development environment should foster exploration of possibilities in a rapid and efficient manner. The new engineering development processes should design approximate system behaviors in a wide range of contexts, which will then be used to explore potential combat advantage by a new level of end-to-end experimentation. The system performance will evolve with *in situ* prototypes, proxy platforms, surrogate areas of responsibility, and hybrid virtual/real system testbedding.[25, 29]

The conventional systems development process currently used in UDNS-1 is not entirely abandoned in the evolutionary context; it is, however, placed in a larger context of an evolutionary process. There is a need to deal with the paradox of flexibility, where a tension exists between the necessity to simultaneously manage change in a dynamic process and still maintain control in dealing with expected engineering progress. Adaptations to the traditional process, therefore, can be made. Acceptable adaptations include the following:[26]

- Incorporate a driving paradigm shift that is overarching to the process, shaping the initial requirements. The paradigm shift incorporates the significant changes in the relationship between system components afforded by distribution and networking.

- Start with provisional general functional requirements as a baseline and justify the elimination of any requirement. This process allows a greater number of options to be explored that may have initially unperceived value.

- Incorporate into the process alternative operational concepts developed through scenario-based coevolution with the warfighter, technologist, and analyst.

- Add operational effectiveness criteria to the evaluation process used in requirements, design, implementation, and testing. Doing so allows for the opportunity to discover unpredictable payoffs and shortfalls.

- Utilize prototyping for control during system development; provide feedback to other parts of the development process.

- Enforce an end-to-end implementation strategy with appropriate feedback loops. Implementation must be reconciled with the realities of performance, cost, and schedule tradeoffs in legacy system integration.

Additional adaptations can be developed by applying key concepts of "enhanced evolutionary engineering," developed by Bar-Yam[26] (see appendix D). These concepts are viewed as insights into early practices in the engineering of UDNS.[25, 28] Evolutionary engineering becomes the overarching systems engineering framework that evolves capability by engineering new sciences into the problem-solving, thus fostering learning-by-doing innovation and enabling adaptation to unexpected changes in the system development and operating environment. The engineering process for complex systems and UDNS, therefore, is ultimately manifested as a continuous learning process.

Evolutionary engineering of military distributed systems, as an innovative and continuous learning process, emphasizes joint experimentation. In the last 10 years, the realities of building a distributed networked joint capability have led to an increase in intellectual rigor, organizational alignment, and field practice of joint experimentation and military innovation.[29, 30, 31] Note that experimentation includes a broad range of possible activity within the context of gaining knowledge of behavior and effects by manipulation of variables for feedback to the evolutionary engineering process: analytic wargames, constructive closed-loop simulation, human-in-the-loop virtual experiments, and field experiments. Even though adequate functional testing of complex engineered systems via M&S is not possible, M&S serves an important role, including experiment scoping, design, decision stimulation, and limited augmentation of live field experiments. For large, resource-intensive, theater-level exercises involving UDNS, results are frequently disappointing because of the lack of opportunities to explore alternate capabilities options for behavior-and-effect comparison. A model-experiment-model paradigm with effective feedback can enhance the utility of exercises and wargames and the overall productivity of the evolutionary engineering process applied to UDNS.[31]

The Department of Defense acquisition system has recently made some changes to align itself with the realities of "system-of-systems" development, but it is generally not aligned with the described evolutionary engineering process.[32] The guideline for program managers for the current "evolutionary acquisition" remains one of top-down rigid requirements, system investments driven by predictive model-based system performance, design performance and cost optimization, and relatively heavy penalties for risk-taking, innovation, and unexpected outcomes in the development process.

Genuine evolutionary aspects of the current acquisition process involve simultaneous M&S of emergent system-of-systems behavior, continuous architectural reconfiguration, and modular open-systems approaches toward fielding incremental capabilities, building on earlier increments to achieve an overall capability. Missing from this construct are those adaptations to the systems engineering process that would allow a fielded capability to benefit from a sufficiently wide range of design contexts, experimentation, and testbedding with feedback to user requirements to ensure better utility of the fielded systems. Until the gap between the current evolutionary acquisition process and the evolutionary engineering process for distributed systems is narrowed, UDNS developers will have to make engineering progress by being mindful of and working between both the legacy and transformational paths shown in figure 3, each of which has its own rule sets, customers, and stakeholders.

Alternative processes to the current acquisition system are emerging. For example, Cares[29] proposes (1) a new emphasis on provisional requirements and mission-need statements, (2) greater attention to manageable complex subsystems associated with tasks scaled for the complex environments where the subsystems will operate, (3) computer M&S and prototype experimentation of the integrated systems that capture new component relationships being created and enable tradeoff analysis between component functionality and the collective characteristics, and (4) greater feedback between experiments.

Engineering educators and practitioners are advancing the systems engineering discipline for complex systems development through new curricula and professional forums. There is more evolutionary engineering research pertaining to human and social considerations in complex system design and development.[33, 34, 35] As the demand for larger scale and more complex systems like UDNS increases, the engineer encounters human, social, political, and managerial interface issues that add risk to the endeavor.

Adoption of enterprise management is a strategic approach for managing the risk associated with very complex interface issues. Enterprises can be defined as highly integrated systems composed of organizations, processes, tools, and methods with multifaceted relationships between boundaries designed to handle complex problems or environments that cannot be handled by more linear organizational constructs.[33, 34] The enterprise management and system engineering communities are being drawn together by two mutually supportive developments:[33]

- Enterprise management architects are finding utility in taking a systems approach to the enterprise, viewing the enterprise as a holistic, yet complex, system, encompassing many views in an integrated framework: organization, process, knowledge, and information technology.

- Conversely, system engineers are finding that successful design of large-scale, complex systems is no longer purely technical; rather, enterprise issues affect the system design and must be taken into account. The nature of the enterprise responsible for the development and implementation can have a significant impact on the outcome of the system being developed.

As UDNS products become more complex involving a greater number of components and subsystems, the need increases for coordinated interdisciplinary teams (as opposed to traditional integrated project teams), enabled by enterprise organizational models that promote coherency of effort amid complex relationships between customers, stakeholders, providers, and suppliers. Thus, just as the UDNS components are engineered to function as a whole for a desired effect, so must the structural units of the enabling engineering enterprise be sufficiently integrated to function together as a whole for a desired effect.

4.2 ENGINEERING TO UDNS-2

The first two steps necessary for the UDNS engineering community to realize Next-Generation USW capabilities are (1) to understand the building blocks that exist in UDNS-1 and then (2) engage in the evolutionary engineering process toward UDNS-2.* Such first steps can be a daunting task for the system developer whose experience is limited to discrete subsystems of UDNS-1 (for example, towed array, torpedo system, or platform combat system). Gaining insights in engineering UDNS-2, however, is possible by describing notional strategies for system functionality based on "universal-good" tasks that are informed by the paradigms and competitive calculus discussed in sections 2.4 and 3.2. Working with candidate system functions cannot replace the rigorous evolutionary systems engineering process, but it may yield insights on how the process can be initiated. The universal-good, system-function strategies (see paragraphs 4.2.1 through 4.2.5) serve to integrate sensibilities for perceived needs in the not-too-distant-future battlespace. These strategies are a starting point and will change as the requirements evolve and perhaps as technology building blocks change over time.

4.2.1 Sensing

Future operational requirements will increasingly tend toward on-demand "call for sensing," where a threshold for fulfilling UDNS utility can be seen over a wide range of the performance, space, and time tradespace. The following notional universal-good sensing strategies should generally contribute to improved operational effectiveness:

- Provide near-surface (<150 m), short-range sensing output with low probability of false alarm (Pfa) and with range performance sufficient for exploitation by adaptable tactics. This function implies the use of traditional low Pfa-design, offboard strategies, such as correlated in-sensor acoustic, magnetic, and/or electric phenomena detections incorporated in a single-sensor element or performed within a forward-deployed sensor field.

- Put mission-essential, offboard sensor signal-processing computing (for example, detection) into the sensor component. In essence, merge the sensing and computing functions within the sensor so that the sensor is a usable information generator and does not need to rely on high-bandwidth networks to convey sensing information, thus preserving C^2 options for the decision-maker.

- Standardize offboard sensor packaging and employment in such a way that, at a minimum, there are options for sensor coupling with legacy and emerging airframes in the battlespace. This packaging enables the trend toward on-demand sensing and suggests design size and weight constraints.

*It is beyond the scope of this report to examine all USW systems and subsystems (the building blocks in UDNS-1) that are fielded and being planned for transition or to describe these systems within the context of a UDNS-2 operations scenario.

- Ensure that offboard sensor power management is sufficient to maintain field endurance for more than a few days to manage demands to DMER[5]. This function necessitates working the tradespace between sensor energy, density, duty cycle, field densities, and more.

- Complement the other sensing strategies with standoff sensing schemes, such as synthetic aperture radar, with sufficient depth penetration and accuracy to allow use with up-close sensors and tactical engagement planning.

4.2.2 Transport

Resource allocation will likely continue to stress the theater commander with a need to work the tradeoffs between getting the right payloads delivered to the relevant locations in a timely manner. Tradespace varies across all scales of payload delivery missions, including information operations, ISR, maritime interdiction, ASUW from under the sea, MIW, and ASW. The following plausible universal-good UDNS-2 transport strategies should generally contribute to improved operational effectiveness:

- Unmanned vehicle (UV) options that enable on-demand delivery of undersea sensor, weapon, and other payloads. This option necessitates, at a minimum, some degree of UV coupling with airframes in the battlespace, which implies some variants with modest size and weight constraints in the design. It also suggests several pedigrees in a family of UVs.

- UV autonomy (for example, autonomy level 2-3, management by consent or exception[36]) sufficient to manage demands of DMER[5], as well as enable collective vehicle search, surveillance, and monitoring of relevant areas of interest. Even small numbers of UDNS-2 UVs operating in concert with modest patrol speeds have the potential to fill a niche for the warfighter, taking the strain off other resources in theater.

- Platform-UV ocean interfacing that enables physical interoperability between UVs and platforms for deployment, retrieval, and payload interchange. Drawing from sealift and land logistics models, payload delivery options expand significantly when cascade-like interfacing between platforms and vehicles is possible.

- UV power management that is sufficient to maintain tactically relevant mission endurance of more than a few days to manage DMER[5] demands. This function necessitates working the tradespace between vehicle energy, density, speed (both cruise and sprint), and payload capacity.

4.2.3 Networking

UDNS-1 requirements for situational awareness and speed of decision-making continue toward increased volume and speed of information exchange between network nodes in the battlespace. In addition, the Navy's FORCEnet and the Office of the Secretary of Defense Global Information Grid are setting necessary standards to deal with the growing complexity of the networked heterogeneous systems that will likely make up many of the UDNS-2 nodes.[37, 38] The networking must be able to operate robustly over a wide range of transmission paths and information exchange environments—from seabed to the air-sea interface to the battle airspace. At the same time, there is a recognized brittleness of the network when it is faced with a deliberate attack that tempers the payoff of information exchange with the vulnerability risk of relying on too much from the network. Many UDNS-2 candidate approaches currently being explored or developed leverage current and emerging information technology and mobile networking strategies in industry. Recent examinations of FORCEnet implementation strategies include:[37]

- Enabling the management of risks to satellite capacity, from surge demand, attack, or weather. Alternative routing functions will demand increased use of unmanned air vehicles as a dynamic relay node capable of working with platforms and other autonomous vehicles above and below the sea surface.

- Utilizing the concept of the FORCEnet Composeable Environment in the network systems engineering to put together provisional system capabilities from the UDNS-2 sensor output, communications, computing, and information packaging for human consumption and action. The Composeable Environment strategy, recognizing the constraints with an *a priori* networking design strategy, relies on the available building blocks from legacy acquisition and fieldable prototypes to create an integrated networking capability. With sufficient discipline in implementing standards for UDNS-2, an array of communications, router, and information exchange configuration options should be available and enable meaningful experimentation for TTP development by the warfighter.

- Enabling sufficient joint and coalition interoperability baseline designs of essential asynchronous transmission and protocols in dealing with the inherent episodic and intermittent nature of some of the underwater and cross-boundary networking scenarios.

4.2.4 Information Fusion, Pattern Recognition, Interpretation, Cognition, and Decision

The decision requirements for UDNS-2 will likely continue the trend to emphasize collaborative, multilevel, parallel, synchronized decision-making done with increased speed, effectiveness, and accuracy. Supporting the decision-making will be information to the warfighter whose creation, collection, access, processing, fusion from multiple sources, content, context, dissemination, and presentation will need to be "information engineered" with the human cognitive functions as a driver. The functions and associated processes may take different forms depending on the role of the human decision-maker. Strategies for information management and consumption with enduring value should relate to other nonmilitary strategies for decision-making—the human cognitive processes being common across tasks, including technical, policy, procedural, and doctrinal aspects. Plausible UDNS-2 strategies may need to be adaptive to allow for the complex adaptive nature of the human cognitive processes. Some universal-good strategies could include:[38]

- Incorporation of adaptive, user-defined information content selection and visualization. Following the trends in the interaction of humans with the internet, allow for broad options of conveying information to the human, while maintaining the integrity of the content and message. This strategy should also include both machine augmentation of human faculties (for example, memory capacity and correlation speed), as well as human augmentation of machine capabilities (for example, prioritization, association, judgment of relevance, and quality).

- Application of tools for dynamic "what-if" analysis in near real time. The ability to convey situational awareness will continue to improve from UDNS-1 levels; however, the inherent uncertainty of the undersea battlespace will demand inferencing by the decision-maker as risk is being managed. Supporting interactive hypothesis management and testing in a rapid manner are also recommended. The use of nonmilitary decision-aid tools for design insights can be helpful and should be considered part of the building-blocks strategy in this area.

4.2.5 Influence

The requirements to shape adversary behavior for advantage, whether by dissuasion, deterrence, or destruction, should continue to be prominent for UDNS-2 for a wide range of threats. Fulfilling the enduring need of offering a greater number of affordable behavior-shaping options beyond the limited choices of today will likely be important for UDNS-2. For UDNS-2, there may be an underlying strategy of going beyond a relatively large torpedo as the primary shaping option under the sea to a theater-weapons-system approach to influence behavior. This strategy will likely mean broadening the inventory of weapons to include a family of lethal and nonlethal weapons; it will also mean broadening the ways and means in which the weapons are brought to bear on the adversary. Plausible influence strategies with a broad and enduring value could include:

- Complementing large torpedoes with smaller, cheaper torpedoes and nonlethal weapons that have sufficient endurance, speed, autonomy, and payload for mission kill, yet are small enough to be coupled with manned and unmanned joint airframes. The value is to create a much larger set of threat vectors on the adversary and increase the adversary's uncertainty.

- Adopting and adapting logistics and maritime security tagging and tracking schemes that include undersea battlespace threats. Schemes that place tracking tags on neutrals or threats, even if intermittently and primitively, have proven to have enduring value for the land and air warfighter in managing theater risk.

- Complementing undersea weapons with battle damage assessment (BDA) sensing so that influence on the adversary can be known by the joint commander for response and management of resources. The need for BDA in UDNS-2 increases as distributed networked approaches to engagements are used because the result of an attack can have an immediate effect on resource allocation if reattack or other response needs to be summoned from the theater force. This strategy is in contrast with a one-on-one platform engagement, which affects only the local platforms involved.

5. SUMMARY

This report has established the framework for the Next-Generation USW mindset and has defined the nature of an undersea distributed networked system for the technologist and the warfighter. Specifically, this report has

- Presented the rationale, inherent advantages, and implications of Next-Generation USW.

- Described UDNS as a key enabler for the Next-Generation USW.

- Explained why engineering UDNS as a complex system is a challenge for the USW technical community that must co-evolve with warfighter concepts of operations.

The challenges to realizing Next-Generation USW and the enabling UDNS are significant. It is hoped that this report contributes to meeting these challenges by helping system developers frame new system functions and relationships that may be added to the "realm of the possible" for the Next-Generation USW warfighter.

6. REFERENCES

1. "Department of Defense Dictionary of Military and Associated Terms," Joint Publication 1-02, 5 January 2007.

2. O. R. Cote, "The Third Battle: Innovation in the U.S. Navy's Silent Cold War Struggle with Soviet Submarines," Massachusetts Institute of Technology Security Studies Program, Cambridge, MA, March 2000.

3. D. F. McCormick, Speech to National Defense Industrial Association Undersea Division, Groton, CT, September 2005.

4. "National Security Strategy of the United States of America," The White House, Washington, DC, March 2006.

5. "National Strategy for Maritime Security," Office of the Secretary of Defense, Washington, DC, September 2005.

6. "Quadrennial Defense Review Report," Office of the Secretary of Defense, Washington, DC, February 2006.

7. "Options for the Navy's Future Fleet," Congressional Budget Office, Washington, DC, May 2006.

8. M. G. Mullen, "FY07 Annual Long-Range Plan for the Construction of Naval Vessels," Washington, DC, 2 February 2006.

9. Chief of Naval Operations, "Navy Strategic Plan in Support of Program Objective Memorandum 08," May 2006.

10. "Naval Operations Concept," Chief of Naval Operations and Commandant U.S. Marine Corps, Washington, DC, 2006.

11. "Anti-Submarine Warfare Concept of Operations for the 21st Century," Chief of Naval Operations Task Force ASW, Washington, DC, January 2005.

12. V. Clark, "Sea Power 21: Projecting Decisive Joint Capabilities," *U.S. Naval Institute Proceedings*, October 2002.

13. "Naval Warfare Development Command ASW Concept" (unpublished), Naval Warfare Development Command, Newport, RI, 2002.

14. J. R. Benedict, "Future Undersea Warfare Perspective," *Johns Hopkins Applied Physics Laboratory Technical Digest*, vol. 21, no. 2, 2000.

15. J. R. Benedict, "The Unraveling and Revitalization of U.S. Navy Antisubmarine Warfare," *Navy War College Review*, vol. 58, no. 2, Spring 2005.

16. M. E. Martin, "Developing a Vision for an 'Out-of-the-Box' Submarine Force and the Technology for Executing It" (unpublished monograph), circa 2000.

17. W. Hughes, *Fleet Tactics and Coastal Combat*, Naval Institute Press, Annapolis, MD, 2000.

18. R. O. Work, "Naval Transformation and the Littoral Combat Ship," Center for Strategic and Budgetary Assessments, Washington, DC, February 2004.

19. J. Cares, R. Christian, and R. Manke, "Fundamentals of Distributed, Networked Military Forces and the Engineering of Distributed Systems," NUWC-NPT Technical Report 11,366, Naval Undersea Warfare Center Division, Newport, RI, 9 May 2002.

20. "Military Transformation – A Strategic Approach," Office of the Secretary of Defense, Office of Force Transformation, Washington, DC, 2003.

21. C. M. Christensen, *The Innovator's Dilemma*, Harvard Business School Press, Boston, MA, 1997.

22. *Systems Engineering Fundamentals*, Defense Acquisition University Press, Ft. Belvoir, VA, January 2001.

23. J. K. Willoughby, "Adaptations to the Systems Engineering Management Process for Projects with Incomplete Requirements," *Proceedings of the 1989 IEEE International Conference on Systems Engineering*, 1989, pp. 197-200.

24. W. B. Rouse, "Engineering Complex Systems: Implications for Research in Systems Engineering," *IEEE Transactions on Systems, Man and Cybernetic*s *– Part C: Applications and Reviews*, vol. 33, no. 2, May 2003.

25. Y. Bar-Yam, *Making Things Work: Solving Complex Problems in a Complex World*, New England Complex Sciences Institute Knowledge Press, Cambridge, MA, 2004.

26. Y. Bar-Yam, "About Engineering Complex Systems: Multiscale Analysis and Evolutionary Engineering," New England Complex Systems Institute, 2005.

27. Y. Bar-Yam, *Dynamics of Complex Systems*, Perseus Books, New York, 1997.

28. W. R. Ashby, *An Introduction to Cybernetics*, Chapman and Hall, London, 1957.

29. J. R. Cares, *Distributed Networked Operations: The Foundations of Network Centric Warfare*, Alidade Press, Newport, RI, 2005.

30. D. R. Worley et al., "Defining Military Experimentation," Institute for Defense Analysis, Alexandria, VA, February 1999.

31. R. A. Kass, "The Logic of Experimentation," Command and Control Research Program (CCRP), Office of the Assistant Secretary of Defense (NII), Washington, DC, May 2006.

32. *Defense Acquisition Guidebook*, Defense Acquisition University, Ft. Belvoir, VA, November 2006.

33. T. Allen, D. Nightingale, and E. Murman, "Engineering Systems: An Enterprise Perspective," Engineering Systems Department, Massachusetts Institute of Technology, Cambridge, MA, March 2004.

34. D. J. Nightingale and D. H. Rhodes, "Enterprise Systems Architecting: Emerging Art and Science within Engineering System," *Massachusetts Institute of Technology Engineering Symposium*, Cambridge, MA, March 2004.

35. B. E. White, "A Complementary Approach to Enterprise Systems Engineering," *National Defense Industrial Association, 8th Annual Systems Engineering Conference*, San Diego, CA, October 2005.

36 Naval Studies Board, *Autonomous Vehicles in Support of Naval Operations*, The National Academies Press, Washington, DC, 2005.

37. "FORCEnet Implementation Strategy," Committee on the FORCEnet Implementation Strategy, Naval Studies Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies, National Academy Press, 2005.

38. "FORCEnet Requirements/Capabilities and Compliance Policy," Deputy Chief of Naval Operations Ltr, Ser N6N7/5U91622 2, 27 May 2005.

39. K. R. Hasslinger and J. R. Pavlos, "Undersea Superiority Through Distributed Systems Supported by Nuclear Powered Submarine Mother Ships," *Submarine Technology Symposium*, Johns Hopkins Applied Physics Laboratory, Laurel, MD, May 2005.

APPENDIX A
CONCEPTUAL NATURE OF NEXT-GENERATION USW CAPABILITIES: AN EXAMPLE*

*Appendix A is an excerpt from reference 13.

INTRODUCTION

A notional concept of operations is useful to illustrate the nature and the potential strength of the Next Generation USW operational concepts. The illustrative concept of operations focuses on ASW support to the Joint Force and is based on stressing area dimensions and tactical times, highly contested area where manned surface and air platforms are well off shore (several hundred nmi), manned submarines are closer but few in number and an extended IPB period was not possible. A FORCEnet distributed system paradigm is assumed.

SENSING

The sensors employed in areas up to several thousand nmi^2 are envisioned to be small, expendable devices that are not wired together. This type of sensor provides greater deployment flexibility [than] current sensors. The sensors are "multi-part systems" in that they are deployed through the use of cascaded means into trip wires, pickets or areas as befitting the operational scenario. The cascade may be from tactical platform to unmanned vehicle to indigenous sensor mobility. This reduction in delivery mechanism size as the sensor moves closer to the intended location eases delivery and provides for greater stealth. For conditions where pre-positioning is not possible, speed is derived from air, surface and sub-surface delivery in descending order. The delivery method is also dependent on the required level of covertness. The sensors are envisioned to be able to determine their location so precision deployment is not necessary.

Classification of the Target of Interest (TOI) occurs at the sensor. New discrimination methods enabled by close range sensors may preclude many of today's classification problems. Use of short range sensors avoids the clutter problem prevalent with long range sensors. The sensors do not provide a continuous stream of data but provide reports of the presence of the TOI and the current location of the sensor. The performance envelope of the sensor provides localization/targeting accuracy consistent with the envisioned neutralization devices.

COMMAND & CONTROL

The TOI reports are provided via FORCEnet. The episodic reports of TOI location are automatically fed into a Cooperative Undersea Engagement component of the FORCEnet (similar in nature to the AEGIS Cooperative Engagement Capability) where a track is automatically built for the TOI and discrimination of any false targets occurs through contextual methods and correlation with above surface sensor contact reports of surface activity. The Cooperative Undersea Engagement component contains the necessary planning and decision aids. A planning aid is used to generate the sensor field density (3D) requirements based on desired probability of detection for a given time period, localization accuracy, and desired track update rate consistent with the operational scenario. Course of Action (COA) versus risk assessments are provided. If enabled by ROE, automated response from distributed neutralization devices occurs via a component similar to the Digital Fires Network. De-confliction, availability and readiness of blue undersea assets occur via FORCEnet. Force level senior management (emplacement, movement and replenishment), target mensuration and engagement [are] enabled with this system.

RESPONSE

In order to provide the Joint Commander with flexible COA, neutralization techniques enable effects-based destruction, degradation, negation or avoidance of the submarine threat. For rapid response, large and/or highly contested areas necessitate the use of loiter or stand-off capability. Loitering capability is provided from "weapon" pods/modules and/or unmanned/autonomous vehicles co-located and distributed within the sensor field. Stand-off capability is from "weapons" launched from any of a variety of tactical platforms, vehicles or pods/modules. Communication with these devices is via FORCEnet.

The "weapons" take the form of kinetic and non-kinetic devices. Destruction of the adversary is from high speed, hard kill devices. Degradation and negation of the submarine's mission execution can take various forms from "spoofing" to mission kill from non-lethal weapons.

SUSTAINMENT

The use of small, simple and expendable sensors greatly aids sustainment. The size makes it easy to stockpile and deliver quantities of sensors. There are many options for operational delivery of the sensors so replenishment, as necessary, is easy. The sensors do not require physical connection into any system.

If the concept works as anticipated, there would be no need for extended IPB. Simply deliver the sensors system when required and utilize a stand-off capability for neutralization. If a longer term capability is required and the sensors exploit innovative discrimination techniques, the sensors can be extremely low powered providing at least a 30 day capability. If a stand-off neutralization capability is utilized, few weapons should be expended.

SURVIVABILITY (SUSCEPTIBILITY AND VULNERABILITY)

Survivability of this concept hinges on the survivability of the sensor rich field. The use of short range sensors and innovative discrimination techniques should reduce the vulnerability to jamming. A sensor should always be in the proximity and thus able to "see" the TOI. The risk associated with emplacing the sensor rich field and neutralization from loitering and/or stand-off devices is low.

APPENDIX B
IMPLICATIONS OF NEXT-GENERATION USW FOR THE SUBMARINE PLATFORM

It is worth examining the implications of Next-Generation USW on the submarine platform, which is explicitly designed to exploit the undersea domain and project combat power from under the sea. The Next-Generation USW warfighting concepts and enabling DNS will benefit significantly from submarine in-theater participation, but perhaps in expanded and new ways.

The implications of Next-Generation USW may be greater for the submarine than for any other existing platform. Surface and air platforms are on a predictable trajectory of coordination and integration afforded by the network and demand by distributed operations. The history of submarine platform utility from the Cold War to the present, however, has not had significant emphasis in distributed operations.[2] Because of their inherent attribute of speed, stealth, and endurance, submarines are most often associated with two fundamental principles of warfare—surprise and deception, giving them both strategic and tactical relevance. Submarine nuclear deterrent indications and warning (I&W) capabilities will continue to be critical for the near future and must not be diluted as the threat landscape continues to evolve. Numerous potential roles, responsibilities, and distributed capabilities for the submarine will be required to have value in the context of Next-Generation USW distributed operations, for example,

- The submarine, with its stealth, endurance, and mobility, is well suited for service to the joint force for precision sniping, surprise strikes, and quick kills—key capabilities that provide the joint commander with options.

- The submarine will continue to have unique utility in preparation of the battlespace: pre-positioning of critical sensors and communications nodes, as well as land attack strike warfare against key targets.

- The submarine will take on the new role of "quarterback" for a large number of unmanned vehicles spread throughout the operating area. As quarterback, the submarine will "manage" that part of the undersea domain that cannot be managed by the main joint force. This role involves coordinating and deconflicting the distributed force elements, "calling the plays" that operate both above and below the surface. The submarine's ability to deliver and interface with key offboard payloads, such as unmanned undersea vehicles (UUVs), unmanned surface vehicles (USVs), unmanned air vehicles (UAVs), and various networked, sea-based sensors and communications systems is valuable as the joint force continues to move in the autonomous system's direction for the "dirty, dumb, and dangerous" missions.

- The submarine will have standoff attack and defense in depth, integral to the joint force.

- The submarine's role should expand to take a greater share of responsibility for force protection and maintenance of the local air and sea superiority.

- The submarine must offer both critical information and covertness (not obtainable by other means) to be managed by the joint force via combined duplex, simplex, and asynchronous communications networking capabilities above and below the sea surface.

- The submarine will be valuable in employing offboard vehicles in numbers, where joint access is denied, to covertly deliver, position, or reposition sensors and systems necessary to establish the early network for follow-on joint operations. These operations can be sensor-to-shooter networks or more simple networks for monitoring and I&W. Of increasing importance is the submarine's ability to covertly provide long-term monitoring and networking of critical intelligence surveillance reconnaissance (ISR) information of maritime traffic and commerce in the areas of counterproliferation and the War on Terror. In this sense, the submarine is viewed as a "preferential node" for joint networked warfare capability that emanates from and exploits the unique aspects of the undersea domain.

- The submarine platform with its long endurance will be essential for the maintenance of the expeditionary networks needed for persistence. This role is particularly critical because robust survivability favors having many small, well-distributed, networked systems rather than having a few large ones. Submarine augmentation will be the hallmark of this Next-Generation USW platform, with autonomous vehicles capable of delivering prepackaged grid elements.

- The submarine will provide support from under the sea for the Marine Corps' operational maneuver from the sea (OMFTS)/ship-to-objective maneuver (STOM), including submarines, submarine-launched/-supported UAVs, UUVs, Advanced Swimmer Delivery System (ASDS), pre-positioned sensors, communications systems, navigation aids, logistics packages, and weapons systems. The submarine and adjunct vehicles can maneuver within the sea, across the seafloor, and in the air above the sea-land interface in locations beyond the reach of other joint assets to provide information critical to planning and maintaining speed and momentum of operations. A wide range of activities by undersea platforms and systems can be performed to support and enable key OMFTS/STOM operations: (1) providing detailed mapping, environmental characteristics, and targeting data; (2) covertly inserting special packages, additional connectivity, and capacity for essential information processing/fusion, and (3) providing a submerged adjunct of the sea base located closer to littoral penetration points than the main surface component for safe havens against harsh nuclear, biological, chemical, and small arms fire conditions.

- The submarine's traditional nuclear strategic deterrence will be expanded to deter adversary pre-emptive action (nuclear and non-nuclear) in the littorals. Knowledge that the amount of power emanating from the sea via the distributed force with the submarine can be sufficiently intense and precise raises the adversary's risk significantly to be a credible deterrence.

There is an inherent deception capability that is leveraged by the potential strike power of the submarine in that the primary source of advantage in distributed networked forces arises from the network effects that are distributed in many dimensions. This capability allows the submarine to summon deception effects for use in a manner and advantage chosen by the clever commander based on evolving conditions.

Hasslinger and Pavlos[39] present novel ways that the nuclear submarine can operate with various UUVs, leveraging the strengths of both to yield capability reach and agility against future threats. They also note that undersea DNS will mean many nontraditional approaches to old and new USW problems, which will stress the current culture. An awareness of the stresses, however, will enable healthy tensions to exist within the USW community. The technical challenges to create the new relationships between the submarine and other distributed subsystems in the DNS are significant and must be understood by the technical, operational, and acquisition communities so that submarine platform capabilities can evolve with the concept of operations and tactics, techniques, and procedures. Technical challenges include:

- <u>Autonomy</u> for endurance, flexibility, and mission diversity.

- <u>Communications</u> enabling collaboration between manned platforms and networking unmanned vehicles.

- <u>Energy storage</u>, including high charging rates to break (at least in part) the "umbilical cord," providing greater autonomy and freedom of maneuver for all of the platforms and vehicles.

- <u>Launch and recovery</u> (ocean interface) sufficient for in-stride operations.

- <u>Command and control</u> for synthesizing the large amount of information expected from the network of sensors and unmanned vehicles.

- <u>New metrics and associated tools</u> for their measurement and analysis to assess undersea capability based on the performance and capability of the overall theater system.

APPENDIX C
FUNDAMENTALS OF DISTRIBUTED NETWORKED SYSTEMS ENABLING DISTRIBUTED NETWORKED MILITARY FORCES[*]

[*] Appendix C is an excerpt from reference 19.

INTRODUCTION

Any system is created from parts. In traditional military systems, most of the parts are physically connected to a relatively small number of larger parts. These parts are in a sense distributed and networked.

The future warfighting concept of a distributed, networked system is different from existing military systems. There are a much larger number of small parts and the greater majority of these parts are not physically connected to the small number of larger parts. Most parts might not be physically connected to another part at all. When this is the case, other types of connections substitute for physical connections. There are, therefore, two basic building blocks of future distributed, networked systems: the parts (generally referred to as "elements") and the connections between the parts. These are defined as follows:

Element: A physical component or part of a distributed, networked system that performs a certain function, such as sensing, information processing, transportation of itself or other elements, etc. Humans, from an abstract perspective, should be considered elements as well, although they are highly capable, unique, and specialized elements. An important conceptual point is that information technology equipment, such as routers, cabling, and computers are physical elements of a system.

Connection: Any interaction between elements or between elements and the external world. Examples of connections include communications links, weapon-target pairings, or logical relations like inter-sensor collaboration. Connections may be via physical or non-physical interactions. For example, there can be non-physical interactions between sensors and sensed objects and physical connections between munitions and targets.

Note that in this context the term "distributed, networked force" becomes synonymous with "distributed, networked system."

BASIC FUNCTIONS

In military applications, the elements and connections (i.e., the components of a distributed, networked force) conspire to fulfill certain functions; these functions might be executed individually or collectively at many different levels within the force. The basic functions of a networked, distributed force are defined as follows:

Sensing: Collecting observations of objects within a sphere of competition as well as observations of the environment. The observations may be obtained passively (by collecting phenomena emanating from objects or the environment) or actively (by causing objects or the environment to emanate phenomena). Direct and indirect forms of sensing objects, phenomena, information, and events are included.

Transport: Providing mobility for elements that might not have their own locomotion or for elements that in certain cases are more efficiently transported by other elements. An example of the latter is transportation of a missile to a launch site. While a missile may possess a vehicular function to propel its warhead, this system may not be suitable for autonomous transport to a firing position.

Netting: Creating the means of information transfer between elements of the system. Information transferred may include the results of sensing functions, transmission of stored data, messages, movement orders or control signals.

Information Fusion and Pattern Recognition: Sharing information among elements for the purpose of collecting observations from sensors, composing informational representations of the battlespace, and determining important patterns within the representations. Information about the non-physical characteristics and behaviors of objects (such as the content of messages) is developed in this function. This includes conversion of raw data into basic information.

Interpretation, Cognition and Decision: Consuming information, deliberating and converting deliberations into decisions. This includes not just the individual deliberations and decisions of commanders but also the collective cognitive activity of an entire command structure.

Influence: Acting to change physical, informational, or logical states in the battlespace. Influence can include physical destruction with weapons, application of nonlethal force, information warfare, or reconfiguration of friendly elements and connections. Influence includes all kinetic and nonkinetic means of obtaining desired effects for various levels of military response.

DEFINING CHARACTERISTICS

Absent some special considerations, one could argue that the basic functions discussed here apply to any military force. If future distributed, networked forces are to provide unique and revolutionary advantages, there must be particular characteristics that result in the improved performance. The following list, based on research into distributed, networked systems in other contexts, is a set of characteristics—a framework—that defines unique synergies and interrelationships expected of future distributed, networked military systems:

- Number of elements and collective behavior
- Connection topology
- Connection strength
- Diversity
- Scale.

The realization of these synergies and relationships is the foundation for performance improvements.

Number of Elements and Collective Behavior

The future distributed, networked system will typically have a large number of elements. Although elements can individually perform the basic functions as defined above, interesting collective behavior begins even when the number of elements is more than two. More complex behaviors develop as the number of elements grows, and networks of tens of elements can exhibit very intricate interactions. Extraordinarily nonlinear "tipping points" can occur when some systems have about 500 elements, but, importantly, the tipping point can disappear with somewhat fewer elements. The same type of system with thousands of elements can cancel out tipping point benefits because of a dramatic increase in command and control overhead. The number of elements and resultant collective behavior will be an important characteristic of future distributed, networked forces.

Connection Topology

A distributed, networked system will typically be well connected; but a maximally connected system (a system in which all elements are directly connected to all others) is hampered by the same kind of ballooning overhead as a system with too many elements. A minimally connected system (one less connection than there are elements—just enough to link all the elements in one group) can be too brittle and vulnerable. Moreover, lattice-type structures (in which each element is connected, say, to exactly three other elements in a regular matrix) can be too rigid. Most real distributed systems (like the internet) have a mix of connection properties, such as preferential attachment (some elements can be more useful to connect with than others), clustering (elements can be functionally collected in local subsets) or path formation (creation of indirect conduits between elements collaborating on certain tasks through intermediary elements and connections). In addition, most real distributed, networked systems assume a specific configuration based on the resources available and the task at hand; they reconfigure as resources or tasks evolve. Note also the dual nature of connections: they are both links between elements that might provide advantage as well as targets for attack. Distributed, networked military systems will likely have a mix of connection properties.

Connection Strength

Of similar importance to the number of elements and the topology of connections is the strength of connections between elements. This characteristic defines the rate and degree of response and adaptation in distributed, networked systems. For example, some systems with weak connections might require very large control signals to reconfigure elements; if connections in the same system are too strong, then very small control signals can cause uncontrollable changes in the system, perhaps even "freezing" the system if too many strong input signals become operative simultaneously. Most distributed, networked systems have a mix of strong and weak connections, the relative strength of which change over time based on system employment. An example of this characteristic in military forces would be the strength of a phenomenon observed by an element with a sensor function. If the element were close to the source of the phenomenon, the connection would be strong, but if the element were more distant from the phenomenon, then the connection would be weak. A sensor investigating multiple phenomena is faced with the dilemma of maintaining weak connections with all targets (and therefore reacting poorly to their behaviors) or abandoning all but one phenomenon to maintain a strong and more reliable connection with one target (forgoing a response to all but the remaining target, with which the sensor is now closely coupled).

Diversity

Another important defining characteristic is the diversity of the elements and connections. Many concepts for distributed, networked military forces depend on mass-production of identical elements, but this Industrial Age approach could backfire in complex applications. Research into distributed, networked systems in other contexts shows that the systems best able to learn and adapt to their competitors and the environment have diverse elements and connections. When elements and connections are highly specialized and standardized (i.e., when there are a decreasing number of types of elements and connections—a decrease in diversity) adaptation is devalued and systems become much more vulnerable to catastrophic failure in rapidly changing, competitive environments. At the other extreme, however, are concepts for systems where almost every element and connection is unique—these systems would require extraordinary overhead to mensurate interactions between elements and connections. Most real distributed, networked systems have a healthy balance between diversity, standardization, and specialization.

Scale

Scale is the extent to which the same system looks different when observed at different levels of resolution. Very few dynamic, competing systems are "scale invariant," meaning that every important behavior can be observed, understood and influenced from any scale of observation. Most dynamic, competing systems are sensitive to scale, meaning that different behaviors occur at different scales. A distributed, networked system will be inefficient (or even completely ineffective) if it cannot observe, understand or influence behaviors at the scales in which they occur. Scale, in this sense, is an important defining characteristic of distributed, networked forces.

DESIGN GOALS OF DISTRIBUTED FORCES

The building blocks, functions, and defining characteristics begin to describe how distributed, networked forces might operate. The next step is to state the basis on which performance in distributed, networked forces should be judged. A clear idea of why advantage matters will help inform how advantage is accrued. These "design goals," each considered universally good for distributed, networked forces, include persistent operational advantage, collective competitive behavior, stable system performance, and dynamic adaptability.

Persistent Operational Advantage

Operational advantage is dependent upon the ability of military forces to adaptively maintain advantageous positions against a clever foe, even when the foe takes surprising initiatives, innovates dramatically, or changes the rules of the game. A distributed, networked force must, therefore, be capable of drawing upon extremely diverse and varied sources of advantage from a finite set of elements and connections. To do this, actions might not always be "optimal," in the strictest sense; they might temporarily admit disadvantage in order to regain a more persistent operational advantage later.

Collective Competitive Behavior

The defining characteristics suggest that centralized control of distributed, networked forces requires far too much overhead to be effective. The ability to act as purposeful collectives without the prescribed, centralized control or synchronization of all elements is a design goal of distributed, networked forces. Moreover, an enemy's ability to discern friendly intent will be dramatically reduced if the macroscopic system actions are not mapped directly or obviously to the actions of the discrete elements. Examples of such behaviors from other contexts include wolf packing, immune system reactions, insect swarm defense, and human crowd dynamics.

Stable System Performance

The competitive environments in which distributed, networked forces operate can be extraordinarily complex and unpredictable. A distributed, networked force must, therefore, have a fundamental precept of stability in the midst of turmoil. This does not mean that the force should be ossified, simple or uninventive, but that it should have the type of dynamic, controllable stability akin to "physical agility," including aspects of "balance." Stable performance implies that the limited loss of elements or connections should not significantly impact the force's macroscopic behavior.

Dynamic Adaptability

The linear branch-and-sequel method of operational planning is inappropriate for the dynamic operational environments in which distributed, networked forces compete. Operators, however, will still be required to perform traditional long-term planning functions such as resource allocation, performance assessment, and operational planning. Since these functions entail the ability to simultaneously allocate, assess, and plan at different time scales and in multiple dimensions, distributed, networked forces must be capable of being simultaneously controlled at a great many scales and in a great many dimensions. The ability for forces and the system to self-synchronize is imperative.

POTENTIAL DESIGN PRINCIPLES

The previous sections have laid out components, functions, dynamics, and value propositions for distributed, networked forces. The sources of advantage in such military systems have been discussed. Confident extrapolations can be made about useful design principles of distributed, networked forces. An initial list of these includes the following.

Recombination: The ability to aggregate, distribute or interchange physical, informational or logical elements and connections. This design principle provides a distributed, networked force that adaptively evolves to the right number of elements, effective connection topology, requisite diversity and appropriate scales of observation and competitive behavior.

Dispersion: Avoiding spatial, informational, or logical centers of gravity while confounding adversary command, control, and scouting resources. This design principle provides one of the most significant contributions to advantage in distributed, networked military systems: advantage can be obscured and protected by dispersal and then marshaled for application.

Mobility: Sufficient speed for rapid relocation of elements and reconfiguration of element collectives through physical or logical means. Mobility provides a repertoire of agile maneuvers for a range of operational situations, nimble dispersal, and quick aggregation.

Stealth: Greater numbers of elements provide physically smaller elements and stealthier signatures. Distributed, networked effects can suggest ways in which smaller elements can improve collective performance yet reduce observability.

Proximity: Most objects in contemporary military systems have such intrinsic value in their physical components that direct proximity to a threat incurs great risk to the platform and, thus, to mission success. Distributed, networked forces can provide a level of proximity dictated by appropriate connection strengths, collective behaviors, and scale considerations. Greater numbers of smaller, stealthier objects, which manifest more of their value in informational and logical contributions than physical combat power, complement the design principle of proximity.

Flexibility: Reliable, fluid system substructures with a wide range of interoperability options. A key aspect of this design principle is robustness of information technology architectures and information management schemes. Adherence to this principle would provide a sustained force stability in a distributed, networked force during vigorous adaptation to radical competitive behaviors or extreme environmental conditions.

Persistence: Ability of forces to operate without disruption by cyclic logistics. A design principle for distributed, networked forces provides a logistics infrastructure that also capitalizes on distributed, networked logistical effects. One manner to achieve this is to *reduce* constraints on logistics and create a more adaptive flow of goods and service (a notion counter to the Joint Vision Concept of Focused Logistics).

APPENDIX D
KEY CONCEPTS IN ENHANCED EVOLUTIONARY ENGINEERING (E^3)*

*Appendix D is an excerpt from reference 26.

FOCUS ON CREATING AN ENVIRONMENT AND PROCESS RATHER THAN A PRODUCT

Ongoing change in a system is the underlying mechanism of creation, not the formulation and execution of plans. Encouraging and safeguarding this ongoing change and monitoring its outcomes are the absolute essentials of an evolutionary-based process.

CONTINUALLY BUILD ON WHAT ALREADY EXISTS

Off-line engineering of complex systems is impractical because the complexities of their environment and true functional requirements do not permit practical specification or testing prior to implementation. In complex systems, correct expectations and testing both depend on the immediate consequences of current operations.

INDIVIDUAL COMPONENTS MUST BE MODIFIABLE *IN SITU*

The interdependencies between system components must be such that individual components can be modified in situ. In practice this requires the following point.

OPERATIONAL SYSTEMS INCLUDE MULTIPLE VERSIONS OF FUNCTIONAL COMPONENTS

Complex systems should be understood as populations rather than as rigid assemblies of unique components. Individual components can overlap substantially in terms of both functionality and interaction. Evolutionary processes impact both populations and individuals. Redundancies are not always unwanted inefficiencies.

UTILIZE MULTIPLE PARALLEL DEVELOPMENT PROCESSES

The existence of populations of components allows multiple parallel efforts to explore modifications that might (but that are not guaranteed) to improve system components and/or total system capability.

EVALUATE EXPERIMENTALLY *IN SITU*

Testing and experimentation increasingly overlap. Off-line qualification testing becomes a prelude to active field testing for components in a large variety of operational environments. Results (including unexpected results) are ratified or rejected as they occur based on then-current overall system capability.

INCREASE UTILIZATION OF MORE EFFECTIVE COMPONENTS, GRADUALLY

The replacement of components cannot be abrupt as testing is never complete and operation is continuous. Augmentation and parallel operation is the preferred approach.

EFFECTIVE SOLUTIONS TO SPECIFIC PROBLEMS CANNOT BE ANTICIPATED

Specification efforts cannot assume that the most efficient or effective solutions can be anticipated in advance of an exploration and discovery process involving multiple parallel development efforts. Such an assumption is invalid, and is increasingly seen to be so the more complex any solution must be to even marginally succeed. Moreover, this assumption remains false no matter how long a problem is worked and progressively better solutions are found.

THE "INTEGRATION" OF COMPLEX SYSTEMS

In order to operate a E3 process, the concept of integration must be radically rethought. A systematic and effective application of the ideas in this paper involves a "paradigm shift" from "complete system specification" to the creation of environments that are conducive to ongoing change in components of systems while supporting the more or less constant evaluation of their overall effectiveness through virtual as well as real world testing.

INITIAL DISTRIBUTION LIST

Addressee	No. of Copies
Office of Naval Research (03R (P. Gruber), 03I, 03T (J. Lawrence), 32 (F. Herr), 32X (D. Johnson) 31 (B. Junker), E. Kapos))	7
Chief of Naval Operations (N00K, N091 (J. Barkley), N3/N5, N60, N61, N71, N71F (Dufresne), N6 Technical Director, N81 (T. Barber, RADM Davenpoert), N86F (RADM Carr), N863 (Capt Dropp), N864, N864A, N866 (Capt Sweigard), N874 (Raff, CAPT Chaffee, N87 (RADM Mauney), N875 (P. Harrigan, M. Beirne, M Orr, J. Zittel))	21
Strategic Studies Group (ADM (Ret) Hogg, W. Glenney (10), R. Wilcox, T. Geiske, A. Krulisch)	14
Naval Postgraduate School (W. Hughes, J. Eagle, S. Gallup, J. Kline, J. Rice, RADM (Ret) Jones)	6
Naval Research Laboratory (E. Franchi, F. Erskine)	2
Naval War College (CNWS, NWC Library, WGD (Capt Siemins, Bundy, Pellegrino, Labrerru, Houston, Price), J. Fitzsimmons)	9
Naval Sea Systems Command (PEO-IWS (Technical Director), PEO-IWS5 (Capt. Davis, C. Cannon, T. Carmean), PEO-SUB (D. McNamara), SEA-05, SEA-05R, SEA-06, SEA-53, SEA-91, SEA-073T (W. Bankhead), WC S&T (S. Mitchell), PEO-C4I and Space (D. Bauman))	13
Naval Surface Center, Dahlgren Division (J. Moreland, A. Tate)	2
Naval Surface Warfare Center, Coastal Systems Center (G. Kekalis, D. Everhart)	2
Naval Air Warfare Center, Aircraft Division (D. Backes)	1
Naval Air Warfare Center, Weapons Division (P. Yates, D. Janiec)	2
Space and Naval Warfare Systems Center San Diego (D. Endicott, E. Hendricks, G. Galdorisi, M. Gmitruk, S. Stewart, G. Davis)	6
Commander, Pacific Fleet (N00ASW (D. Yoshihara, W. Pittsley), G. Hackney)	3
Center for Security Forces (N8 Science Advisor (E. Spigel)	1
Naval Warfare Development Command, Newport (N00T (W. Perras), P. St. Jacques)	2
Commander Fleet Forces Command (N8 Science Advisor)	1
Commander, Naval Network War Command (N8 (P. Jackson))	1
Office of the Secretary of Defense Office of Net Assessment (A. Marshall, J. Raymond)	2
Office of the Assistant Secretary of Defense (ASD-NNI (Deputy/CHENG))	1
Joint Forces Command (J9, JFCOM/MITRE (R. Richards))	2
Defense Advanced Research Projects Agency (STO (D. Honey, B. Pierce, L. Stotts, K. Latt, E. Carapezza), TTO (S. Welby, S. Walker), IXO (R. Tenny, M. Davis, A. Moshvegh)	10
Center for Naval Analysis (H. Spivack, R. Poore)	2
Institute for Defense Analyses (J. Hanley)	1
Johns Hopkins University/Applied Physics Laboratory (J. Benedict, VADM (Ret.) J. Fitzgerald, D. Tyler, W. LaPlante, R. Mitnick, L. Green, R. Henrick)	7
RAND Corporation	1
The MITRE Corporation (S. Starr)	1
Alidade Inc. (J. Cares, B. Braswell, J. Dickman)	3
Massachusetts Institute of Technology Center for International Studies (Security Studies Program)	1

INITIAL DISTRIBUTION LIST (Cont'd)

Addressee	No. of Copies
Massachusetts Institute of Technology (A. Baggeroer)	1
Office of the Under Secretary of Defense (DDR&E (T. Pudas))	1
Navy Mine and ASW Command (J. Fergusan, S. Pelstring, D. Thigpen)	3
Defense Technical Information Center	2